Joint 48th IEEE Conference on Decision and Control and
28th Chinese Control Conference
Shanghai, P.R. China, December 16-18, 2009

Indirect Coupled Oscillators for Keystream Generation in Secure Chaotic Communication

Rupak Kharel, K. Busawon and Z. Ghassemlooy, Senior *Member, IEEE*

***Abstract*—In this paper, we propose a secure communication system composed of four chaotic oscillators. Two of those oscillators are unidirectionally coupled and employed as transmitter and receiver. The other two oscillators are indirectly coupled and are employed as keystream generators. The novelty lies in the generation of the same chaotic key both in the transmitter and receiver side for encryption and decryption purposes. We show, in particular, that it is possible to synchronize the two keystream generators even though they are not directly coupled. So doing, an estimation of the keystream is obtained allowing decrypting the message. The performance of the proposed communication scheme is shown via simulation using Chua and the Lorenz oscillators.**

I. Introduction

THE importance of chaotic synchronization for the development of secure communication systems is well-understood by now [1-6]. In recent years, various chaotic synchronization methods have been proposed [3-5, 7, 8] together with a number of modulation methods for chaotic communication systems such as chaotic masking [1, 5], parameter modulation techniques [5], chaotic shift keying [2, 5], just to mention a few. Each of these methods requires chaotic synchronization for message extraction at the receiver side. On the other hand, different attacks methods have been derived in order to test the security of the modulation methods; namely the non-linear dynamics forecasting [9, 10], return maps analysis [11], artificial neural network analysis [12] and so on. As a result, methods like chaotic masking, parameter modulation techniques and chaotic shift keying were found not to be secure.

In [6], a method based on encryption technique was proposed, where a different output from chaotic transmitter which was transmitted in the channel was used as a keystream to encrypt the message signal. The encrypted message signal masked with another output of the chaotic oscillator was employed as the transmitted signal. It was claimed that since the intruder could not get hold of the keystream, it was impossible for the attackers to extract the message. But a later work done by Parker & Short [13] showed that it was still possible to extract the keystream from the transmitted chaotic signal since the keystream carried the information of the dynamics of the transmitter. In fact, since, both the carrier and keystream were the outputs of same oscillator; the carrier held the dynamics of the keystream as well. Therefore, it was impossible to hide the dynamics of the keystream from intruders, as a signal has to be transmitted from the transmitter to the receiver for synchronization and message transmission purpose. However, since the method proposed in [6] is nevertheless interesting, there is a real incentive for finding ways for improving the method by eliminating its shortcomings.

In effect, in this paper, based on the spirit of the work in [6], we propose a new chaotic communication scheme composed of four chaotic oscillators. Two of those oscillators are unidirectionally coupled and employed as transmitter and receiver. The other two oscillators are indirectly coupled and are employed as keystream generators. The key idea therefore is to generate a chaotic carrier signal from one oscillator while chaotic keystream is generated from another chaotic oscillator. A suitable encryption rule is employed in order to encrypt the message using the generated keystream. The encrypted message is then modulated with the chaotic carrier in order to generate the transmitted signal. As a result, the transmitted signal does not contain the dynamics of the keystream oscillator, hence making it difficult for intruders to generate the keystream with the sole knowledge of transmitted chaotic carrier. At receiver, the same keystream is generated and decryption rule is applied to the recovered encrypted message signal which is obtained from chaotic synchronization. However, an obvious question arises: *is it possible to synchronize two independent chaotic oscillators such that they generate same required keystream*? It will be shown in the next section that, under some assumptions, it is still possible to synchronize two chaotic oscillators even though they are not uni-directionally coupled.

An outline of the paper is follows: In Section II, the main methodology of the proposed technique will be explained and indirect coupled synchronization is proven for a class of chaotic system. In Section III, implementation of the proposed synchronization technique and proposed secure chaotic communication technique will be implemented using the Lorenz system and Chua's system. In Section IV, simulation will be carried out and results will be shown. Finally in Section V, concluding remarks will be made.

II. The Proposed Communication System

The proposed chaotic communication, based on cryptography, is shown in Fig. 1. The novelty here lies in the

Manuscript received March 3, 2009. This work was supported by Northumbria University.

Rupak Kharel, Krishna Busawon and Z. Ghassemlooy are with School of Computing, Engineering and Information Sciences, Northumbria University, Ellison Building, Newcastle upon Tyne, NE1 8ST, UK. (Corresponding author email: rupak.kharel@unn.ac.uk).

generation of the keystream. The chaotic transmitter (T) is first used to generate two output signals, $y_1(t)$ and $y_2(t)$. The signal $y_1(t)$ is used for modulation purpose while output $y_2(t)$ is used to drive chaotic oscillator (A) with a different structure than the transmitter (T). The output $k(t)$ of key generator (A) is used as a keystream to encrypt the message $m(t)$ using an encryption rule $\phi(.)$. The resulting encrypted signal $\phi(m(t))$ is masked using $y_1(t)$ yielding the transmitted signal $y_t(t)$. The output $y_t(t)$ is fed back into the transmitter in the form of an output injection with the aim of reducing the effect of non-linearity while performing synchronization at the receiver side. The modulated transmitted signal $y_t(t)$ is sent through the channel to the receiver.

At the receiver end, upon receiving the signal $y_t'(t)$, the chaotic receiver (R) - which is similar in structure to the transmitter (T) - permits to obtain an estimate $\hat{y}_1(t)$ and $\hat{y}_2(t)$of the signals $y_1(t)$ and $y_2(t)$ respectively by synchronization. This can be done by using any techniques existing in the literature [3, 4, 7, 8]. The signals $\hat{y}_1(t)$ and $y_t^{'}(t)$ are used to generate an estimate $\hat{\phi}(m(t))$ of the encrypted signal $\phi(m(t))$. The estimate $\hat{y}_2(t)$ is used to drive the chaotic key generator (B) - which is similar in structure to generator (A) - which yields the keystream estimate $\hat{k}(t)$. Consequently, the message $m(t)$ can be recovered by using the decryption rule $\phi^{-1}(.)$.

Note that since, the chaotic key generators (A) and (B) are driven by $y_2(t)$ and $\hat{y}_2(t)$ respectively, an indirect coupled synchronization is required between these two chaotic oscillators. Also, $y_2(t)$ and $\hat{y}_2(t)$ are outputs of chaotic transmitter (T) and receiver (R) respectively and will be equal once synchronization is obtained. Intuitively, one would expect this synchronization to take place. However, we will prove this mathematically for a class of chaotic systems.

The important part of this method is the generation of the keystream. No information regarding the keystream is transmitted in the channel. In [6], it was possible to estimate the state which was used as keystream (as shown in [13]) since the state that was transmitted in the channel had some information of the dynamics of the keystream as they were state variables of same chaotic oscillator.

In contrast, in this method, the keystream is generated from a chaotic oscillator with a totally different structure. It will not be possible to estimate the dynamics of the chaotic key generator from the signal being transmitted in the channel by using the method mentioned in [13]. Even if the intruder manages to get the encrypted signal from the transmitted signal, without the knowledge of keystream, the message signal could not be decrypted back. Therefore, a secure communication link can be realized by implementing the proposed method.

Based on the communication scheme illustrated by Fig. 1, we assume that the transmitter oscillator (T) described by a dynamical system of the following form:

$$(\mathrm{T}):\begin{cases}\dot{x} = \mathbf{A}(y_t)x + b(t, y_t)\\ y_1 = h_1(x)\\ y_2 = h_2(x)\\ y_t = y_1 + \phi(m,k),\end{cases} \tag{1}$$

where the state $x \in \mathbb{R}^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator $y_1 \in \mathbb{R}$ and $y_2 \in \mathbb{R}$. The matrix $\mathbf{A}$ is of appropriate dimension while h_1 and h_2 are analytical function vectors of appropriate dimensions. The signal $y_t \in \mathbb{R}$ is the transmitted signal where $\phi(.)$ is the encryption function using key $k(t)$ and the function b is a smooth bounded function of time.

The keystream $k(t)$ is generated using another chaotic oscillator of similar form as above but is driven by the output $y_2(t)$ that is:

$$(\mathrm{A}):\begin{cases}\dot{z} = \mathbf{F}(y_2)z\\ k = h(z),\end{cases} \tag{2}$$

where $z \in \mathbb{R}^q$ (q is not necessarily equal to n), $k \in \mathbb{R}$ is the keystream and h is an analytical function vector of appropriate dimension. It is assumed that the channel is perfect and that no distortion of the transmitted signal has

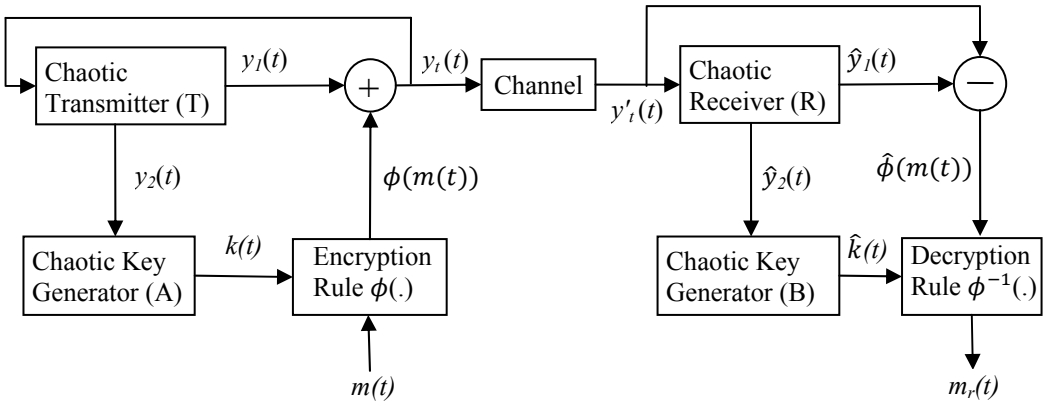

Fig. 1. Block diagram of the proposed chaotic communication based on cryptography.

taken place; that is $y_t = y'_t$.

The receiving chaotic oscillator (R) is given by:

$$(\mathrm{R}):\begin{cases}\dot{\hat{x}} = \mathbf{A}(y_t)\hat{x} + b(t, y_t)\\ \hat{y}_1 = h_1(\hat{x})\\ \hat{y}_2 = h_2(\hat{x}),\end{cases} \tag{3}$$

Finally, the key generator (B) is given by:

$$(\mathrm{B}):\begin{cases}\dot{\hat{z}} = \mathbf{F}(\hat{y}_2)\hat{z}\\ \hat{k} = h(\hat{z}),\end{cases} \tag{4}$$

We shall make the following assumptions:

A1) The output y_1 of transmitter (T) is flat,

A2) There exist symmetric positive definite (SPD) matrices $\mathbf{P}_1$, $\mathbf{P}_2$, $\mathbf{Q}_1$ and $\mathbf{Q}_2$ such that for all $\xi \in \mathbb{R}$,

$$\begin{aligned}\mathbf{A}^{\mathrm{T}}(\xi)\mathbf{P}_1 + \mathbf{P}_1\mathbf{A}(\xi) &= -\mathbf{Q}_1\\ \mathbf{F}^{\mathrm{T}}(\xi)\mathbf{P}_2 + \mathbf{P}_2\mathbf{F}(\xi) &= -\mathbf{Q}_2.\end{aligned} \tag{5}$$

A3) There exist a positive constant $\nu \geq 0$ such that $\left\|\mathbf{F}(\xi) - \mathbf{F}(\hat{\xi})\right\| \leq \nu\left\|\xi - \hat{\xi}\right\|$, and

A4) The output function $h_2(x)$ is globally Lipschitzian with respect to x.

The objective is to show that the transmitter (T) and the receiver (R) synchronize as well as generators (A) and (B) are synchronized with each other even though there is no direct link between them. In effect, based on the above assumptions, we state the following:

Theorem 1. *Under the assumptions A1) and A2), there exist two constants* $\lambda, \eta > 0$ *such that* $\left\|x(t) - \hat{x}(t)\right\| \leq \eta e^{-\lambda t}\left\|x(0) - \hat{x}(0)\right\|$ *for all* $t \geq 0$. *In other words, the receiver (R) synchronizes exponentially with the transmitter (T).*

Proof: Let $\varepsilon(t) = x(t) - \hat{x}(t)$, then the error dynamics between transmitter (T) and receiver (R) is given by:

$$\dot{\varepsilon} = \mathbf{A}(y_t)\varepsilon. \tag{6}$$

Owing to assumption A2), a candidate Lyapunov function of the above error dynamics can be chosen as:

$$V(\varepsilon) = \varepsilon^T\mathbf{P}_1\varepsilon. \tag{7}$$

Differentiating $V(\varepsilon)$ with respect to time, yields:

$$\begin{aligned}\dot{V}(\varepsilon) &= \dot{\varepsilon}^T\mathbf{P}_1\varepsilon + \varepsilon^T\mathbf{P}_1\dot{\varepsilon}\\ &= \varepsilon^T\left[\mathbf{A}^T(y_t)\mathbf{P}_1 + \mathbf{P}_1\mathbf{A}(y_t)\right]\varepsilon = -\varepsilon^T\mathbf{Q}_1\varepsilon.\end{aligned} \tag{8}$$

Since $\mathbf{Q}_1$ is SPD, there exist, $c_1, c_2 > 0$ such that $c_1\varepsilon^T\mathbf{P}_1\varepsilon \leq \varepsilon^T\mathbf{Q}_1\varepsilon \leq c_2\varepsilon^T\mathbf{P}_1\varepsilon$. Consequently,

$$\dot{V}(\varepsilon) = -c_1V(\varepsilon).$$

Integrating the last equation results in:

$$V(\varepsilon(t)) = e^{-c_1t}V(\varepsilon(0)).$$

Again, since $\mathbf{P}_1$ is SPD, there exist $\lambda_1, \lambda_2 > 0$ such that $\lambda_1\varepsilon^T\varepsilon \leq \varepsilon^T\mathbf{P}_1\varepsilon \leq \lambda_2\varepsilon^T\varepsilon$. Consequently:

$$\lambda_1\left\|\varepsilon(t)\right\|^2 \leq \lambda_2 e^{-c_1t}\left\|\varepsilon(0)\right\|^2.$$

In other words:

$$\left\|\varepsilon(t)\right\| \leq \sqrt{\frac{\lambda_2}{\lambda_1}}e^{-\frac{c_1}{2}t}\left\|\varepsilon(0)\right\| = \eta e^{-\lambda t}\left\|\varepsilon(0)\right\|. \tag{9}$$

That is:

$$\left\|x(t) - \hat{x}(t)\right\| \leq \eta e^{-\lambda t}\left\|x(0) - \hat{x}(0)\right\|. \tag{10}$$

This means that $\hat{x}(t)$ converges to $x(t)$ exponentially. In other words, the receiver (R) synchronizes exponentially with the transmitter (T). This completes the proof of Theorem 1.

Theorem 2. *Assume that system (A) and (B) satisfies assumptions A1) and A2), then* $\lim_{t\to\infty}\left\|z(t) - \hat{z}(t)\right\| = 0$. *That is, the keystream generator (A) synchronizes asymptotically with the keystream generator (B).*

Proof: Set $\varepsilon(t) = z(t) - \hat{z}(t)$, then the error dynamics between the keystream generator (A) and generator (B) is given by:

$$\begin{aligned}\dot{\varepsilon} &= \mathbf{F}(y_2)z - \mathbf{F}(\hat{y}_2)\hat{z}\\ &= \mathbf{F}(\hat{y}_2)\varepsilon + \left[\mathbf{F}(y_2) - \mathbf{F}(\hat{y}_2)\right]z.\end{aligned} \tag{11}$$

Now consider the keystream generator (A).

$$\dot{z} = \mathbf{F}(y_2)z.$$

It is clear that owing to assumption A2) that (A) is exponentially stable. More precisely, consider the following candidate Lyapunov function:

$$W(z) = z^T\mathbf{P}_2z. \tag{12}$$

Differentiating $W(z)$ with respect to time results in:

$$\dot{W}(z) = \dot{z}^T\mathbf{P}_2z + z^T\mathbf{P}_2\dot{z} = -z^T\mathbf{Q}_2z.$$

By proceeding as above, one can show that there exist two positive constants $\bar{\sigma}$ and θ such that:

$$\|z(t)\| \le \bar{\sigma} e^{-\theta t} \|z(0)\|.$$

Let us study the stability of the error dynamics:

$$\dot{\varepsilon} = \mathbf{F}(\hat{y}_2)\varepsilon + \left[\mathbf{F}(y_2) - \mathbf{F}(\hat{y}_2)\right] z.$$

For this consider the following candidate Lyapunov function:

$$Y(\varepsilon) = \varepsilon^T \mathbf{P}_2 \varepsilon.$$

By differentiating $Y(\varepsilon)$ with respect to time, we obtain:

$$\begin{aligned} \dot{Y}(\varepsilon) &= \dot{\varepsilon}^T \mathbf{P}_2 \varepsilon + \varepsilon^T \mathbf{P}_2 \dot{\varepsilon} \\ &= -\varepsilon^T \mathbf{Q}_2 \varepsilon + 2\varepsilon^T \mathbf{P}_2 \left[\mathbf{F}(y_2) - \mathbf{F}(\hat{y}_2)\right] z \\ &\le -\varepsilon^T \mathbf{Q}_2 \varepsilon + 2\|\mathbf{P}_2 \varepsilon\| \|\mathbf{F}(y_2) - \mathbf{F}(\hat{y}_2)\| \|z\|. \end{aligned} \tag{13}$$

Since $\mathbf{Q}_2$ is SPD, there exist, $a_1, a_2 > 0$ such that $a_1 \varepsilon^T \mathbf{P}_2 \varepsilon \le \varepsilon^T \mathbf{Q}_2 \varepsilon \le a_2 \varepsilon^T \mathbf{P}_2 \varepsilon$. On the other hand it can easily be shown that $\|\mathbf{P}_2 \varepsilon\| \le c_0 \sqrt{Y(\varepsilon)}$ where c_0 is the conditioning number of $\mathbf{P}_2$.

Also due to Assumption A3), we have:

$$\|\mathbf{F}(y_2) - \mathbf{F}(\hat{y}_2)\| \le \nu \|y_2 - \hat{y}_2\| = \nu \|h_2(x) - h_2(\hat{x})\|.$$

Consequently, due to Theorem 1 and Assumption A4), we deduce that there exist some constant $\rho > 0$ such that:

$$\|\mathbf{F}(y_2) - \mathbf{F}(\hat{y}_2)\| \le \rho \|x - \hat{x}\| = \rho \eta e^{-\lambda t} \|x(0) - \hat{x}(0)\|.$$

Finally:

$$\dot{Y}(\varepsilon) \le -a_1 Y(\varepsilon) + 2\bar{\sigma} c_0 \sqrt{Y(\varepsilon)} \rho \eta e^{-(\lambda+\theta)t} \|\varepsilon(0)\| \|z(0)\|.$$

Since $\dot{Y}(\varepsilon) = 2\sqrt{Y(\varepsilon)}\, \dot{\sqrt{Y(\varepsilon)}}$, we obtain

$$\dot{\sqrt{Y(\varepsilon)}} \le -\frac{a_1}{2} \sqrt{Y(\varepsilon)} + \bar{\sigma} c_0 \rho \eta e^{-(\lambda+\theta)t} \|\varepsilon(0)\| \|z(0)\|.$$

The last equation is linear in $\sqrt{Y(\varepsilon(t))}$. Consequently, it can easily be integrated to show that:

$$\lim_{t \to \infty} \sqrt{Y(\varepsilon)} = \lim_{t \to \infty} \|z(t) - \hat{z}(t)\| = 0. \tag{14}$$

Since the right hand side term of the last inequality tend to zero as $t \to \infty$. This completes the proof of Theorem 2. Once the synchronization is obtained between (A) and (B), the message can be decrypted by applying the keystream.

III. APPLICATION OF THE PROPOSED TECHNIQUE USING THE CHUA AND THE LORENZ OSCILLATORS

In this section, the performance of the proposed communication system is demonstrated using the normalized Chua system as the transmitter (T) and the receiver (R). More specifically, (T) and (R) are chosen as:

$$(\mathrm{T}): \begin{cases} \dot{p} = \alpha(q - p - f(y_t)) \\ \dot{q} = y_t - q - s \\ \dot{s} = -\beta q - \gamma s \\ y_1 = p \\ y_2 = s \\ y_t = y_1 + \phi(m,k). \end{cases} \tag{15}$$

$$(\mathrm{R}): \begin{cases} \dot{\hat{p}} = \alpha(\hat{q} - \hat{p} - f(y_t)) \\ \dot{\hat{q}} = y_t - \hat{q} - \hat{s} \\ \dot{\hat{s}} = -\beta \hat{q} - \gamma \hat{s} \\ \hat{y}_1 = \hat{p} \\ \hat{y}_2 = \hat{s}. \end{cases} . \tag{16}$$

The non-linear function $f(\cdot)$ is a piecewise linear function given as:

$$f(\psi) = G_b \psi + 0.5(G_a - G_b)(|\psi + 1| - |\psi - 1|).$$

Note that (15) and (16) are in the form (1) and (3) respectively with $\mathbf{A}(y_t)$ and $b(t, y_t)$ given as:

$$\mathbf{A}(y_t) = \begin{pmatrix} -\alpha & \alpha & 0 \\ 0 & -1 & -1 \\ 0 & -\beta & -\gamma \end{pmatrix}, b(t, y_t) = \begin{pmatrix} -\alpha f(y_t) \\ y_t \\ 0 \end{pmatrix}.$$

It can also be shown that Assumption A2) is satisfied for the following matrices $\mathbf{P}_1$ and $\mathbf{Q}_1$:

$$\mathbf{P}_1 = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \& \mathbf{Q}_1 = \begin{pmatrix} 2\alpha l_1 & -\alpha l_1 & 0 \\ -\alpha l_1 & l_2 & 0 \\ 0 & 0 & 2\gamma l_3 \end{pmatrix}, \tag{17}$$

where $l_1, l_2, l_3, \alpha > 0$, $\beta < 0, \gamma \ge 0$, $l_2 = -\beta l_3$ and $0 < l_1 < \frac{4}{\alpha} l_2$.

By performing successive time derivative of p it can also be shown that A1) is satisfied. Finally, it is obvious that A4) is satisfied. For the key generating oscillators A and B, the Lorenz system defined as is adopted:

$$(A):\begin{cases}\dot{u}=-\sigma u+\sigma v\\ \dot{v}=-20y_t w+ry_t-v\\ \dot{w}=5y_t-bw\\ y=k=d_0u\end{cases}, \quad (18)$$

$$(B):\begin{cases}\dot{\hat{u}}=-\sigma u+\sigma v\\ \dot{\hat{v}}=-20\hat{y}_t w+r\hat{y}_t-v\\ \dot{\hat{w}}=5\hat{y}_t-bw\\ \hat{y}=\hat{k}=d_0\hat{u}\end{cases}. \quad (19)$$

Again it can easily be seen that (18) and (19) are in the form (2) and (4) with $\mathbf{F}(y_t)$ given as:

$$\mathbf{F}(y_t)=\begin{pmatrix}-\sigma & \sigma & 0\\ 0 & -1 & -20y_t\\ 0 & 5y_t & -b\end{pmatrix}.$$

For these systems Assumption A2 hold true for the following choice of matrices $\mathbf{P}_2$ and $\mathbf{Q}_2$:

$$\mathbf{P}_2=\begin{pmatrix}l_1 & 0 & 0\\ 0 & l_2 & 0\\ 0 & 0 & l_3\end{pmatrix}\ \&\ \mathbf{Q}_2=\begin{pmatrix}2\sigma l_1 & -\sigma l_1 & 0\\ -\sigma l_1 & 2l_2 & 0\\ 0 & 0 & 2bl_3\end{pmatrix}, \quad (20)$$

where $l_1,l_2,l_3,\sigma,b,r>0$, $l_2=-\frac{1}{4}l_3$ and $0<l_1<\frac{4}{\sigma}l_2$.

Remark 1. Note that, at first sight one would expect the matrices $\mathbf{P}_2$ and $\mathbf{Q}_2$ to be time dependent since $\mathbf{F}(y_t)$ is time dependent. However, interestingly, due to the particular form of $\mathbf{F}(y_t)$ the matrices turn out to be constants.

The encryption function $\phi(.)$ used is a *n*-shift cipher algorithm given as: (as used in [6]):

$$\phi(m(t))=\underbrace{f_1(...f_1}_{n}(f_1(m(t),\underbrace{k(t),k(t),...,k(t)}_{n})), \quad (21)$$

where $f_1(.,.)$ is a non-linear function given by:

$$f(m,k)=\begin{cases}m+k+2h, & \text{for } -2h\le m+k\le -h\\ m+k, & \text{for } -h\le m+k\le h\\ m+k-2h, & \text{for } h\le m+k\le 2h\end{cases}, \quad (22)$$

with *h* being an encryption parameter which is chosen such that *m* and *k* lie within the interval $[-h,h]$.

Once the keystream generator (A) synchronizes asymptotically with generator (B), the message $m(t)$ can be recovered using a decryption rule corresponding to the encryption rule and which is given by:

$$\begin{aligned}m_r(t)&=\phi^{-1}(\hat{\phi}(m(t)))\\ &=\underbrace{f_1(...f_1}_{n}(f_1(\hat{\phi}(m(t)),-\underbrace{\hat{k}(t),-\hat{k}(t),...,-\hat{k}(t)}_{n})).\end{aligned} \quad (23)$$

where $\hat{k}(t)$ is the estimated key stream and $\hat{\phi}(m(t))=y_t-\hat{y}_1$.

In the next section, simulations are carried out using Matlab/Simulink and it will be shown that the proposed method is able to synchronize satisfactorily and extract the message successfully.

IV. SIMULATION RESULTS

The parameters employed in equation (15,16,18 and 19) are as follows:

$$\sigma=16, r=45.6, b=4.2, \alpha=10, \beta=-14.87$$
$$\gamma=0, G_a=-1.27, G_b=-0.68, d_0=0.05.$$

The encryption parameter h is chosen to be 0.3 and the message $m(t)=0.1\sin(2\pi t)$. Also in encryption rule (21), a 30-shift cipher is used. The initial conditions for each oscillator are chosen to arbitrarily different.

Fig. 2 shows the autocorrelation function of the keystream signal $k(t)$. It is clear that the keystream is not similar to itself with any amount of time shift so its autocorrelation function has only a single spike at point of zero time shift. This means the keystream generated is chaotic in nature and therefore has limited predictability. Fig. 3 shows the encrypted message signal using (21) and signal $k(t)$ as keystream. Fig. 4 depicts the transmitted chaotic carrier and it can be seen that message signal is totally buried inside it.

Fig. 5 illustrates the error in estimating the keystream and it can be seen that although two oscillators are starting from different initial conditions, the error converges rapidly to zero after some initial period taken for synchronization.

Fig. 6 shows the performance of the proposed method in decrypting the message signal back and it is readily seen that the transmitted message signal has been estimated convincingly.

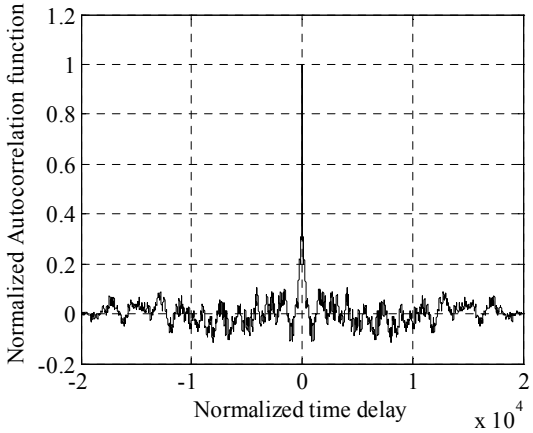

Fig. 2. Autocorrelation of key stream signal *k*(*t*).

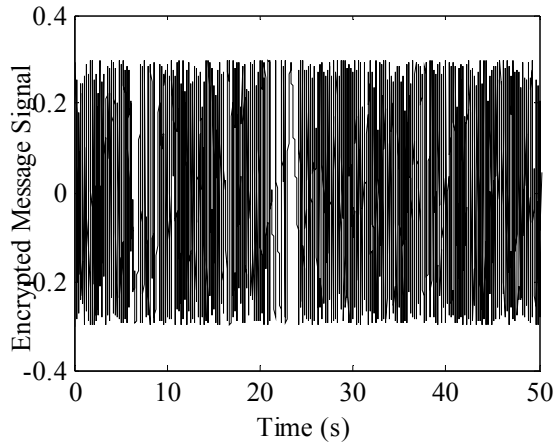

Fig. 3. Encrypted message signal $\phi(m(t))$.

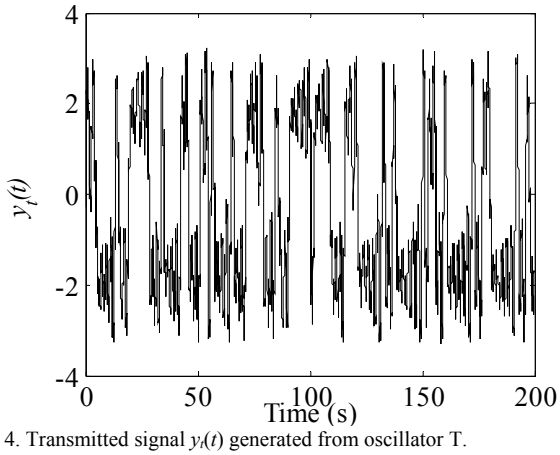

Fig. 4. Transmitted signal $y_t(t)$ generated from oscillator T.

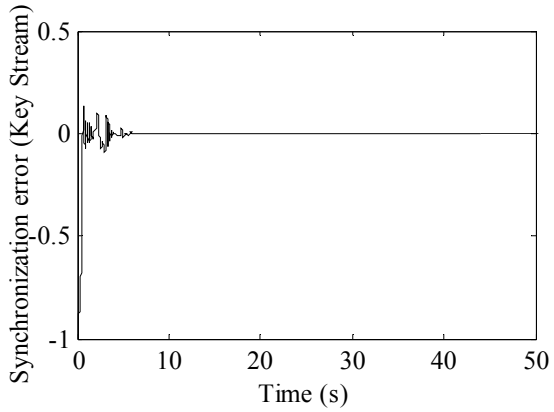

Fig. 5. Synchronization error in estimation of keystream.

V. CONCLUSION

In this paper, a method of synchronizing two chaotic oscillators that are not directly coupled together in a master-slave configuration is proposed and applied to generate the keystream at transmitter and receiver. Synchronization is proven mathematically and simulation results are presented. The main advantage of the proposed method is that, unlike previous work on the topic, the keystream is generated from a different oscillator to that of the transmitter and hence improving the security of the system; since the transmitted signal does not include the information of the dynamics of the key generator. Consequently, even if the encrypted signal is known to the intruders, without the knowledge of the keystream extraction of the message signal will not be possible providing secure communication link.

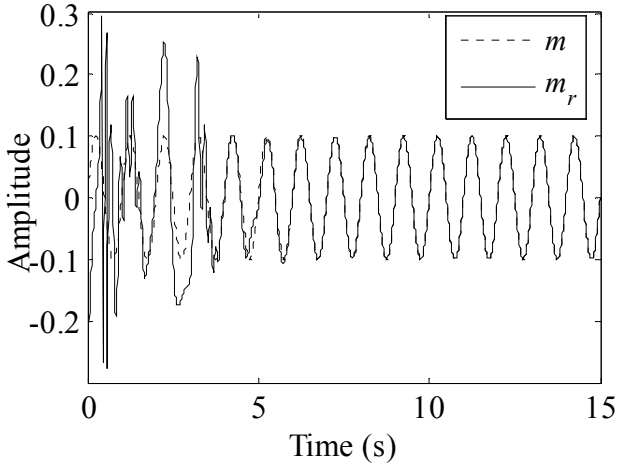

Fig. 6. Plot of the extracted message $m_r(t)$ and $m(t)$.

REFERENCES

[1] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.,* vol. 71, pp. 65-68, 1993.

[2] L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos,* vol. 2, pp. 973-977, 1992.

[3] M. L'Hernault, J.-P. Barbot, and A. Ouslimani, "Feasibility of Analog Realization of a Sliding-Mode Observer: Application to Data Transmission," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 55, pp. 614-624, 2008.

[4] O. Morgul, E. Solak, and M. Akgul, "Observer based chaotic message transmission," *International Journal of Bifurcation and Chaos.,* vol. 13, pp. 1003-1017, 2003.

[5] T. Yang, "A survey of chaotic secure communication systems," *International Journal of Computational Cognition,* vol. 2, pp. 81-130, 2004.

[6] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications,* vol. 44, pp. 469-472, 1997.

[7] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications,* vol. 38, pp. 453-456, 1991.

[8] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," *IEEE Transactions on Circuits and Systems - I: Fundamental thoery and applications,* vol. 44, pp. 882-890, 1997.

[9] K. M. Short, "Steps toward unmasking secure communications," *International Journal of Bifurcation and Chaos,* vol. 4, pp. 959-977, 1994.nthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[10] K. M. Short, "Unmasking a modulated chaotic communications scheme," *International Journal of Bifurcation and Chaos,* vol. 6, pp. 367-375, 1996.

[11] T. Yang, L. B. Yang, and C. M. Yang, "Cryptanalyzing chaotic secure communication using return maps," *Physics Letters A,* vol. 245, pp. 495-510, 1998.

[12] T. Yang, L. B. Yang, and C. M. Yang, "Application of neural networks to unmasking chaotic secure communication," *Physica D,* vol. 124, pp. 248-257, 1998.

[13] A. T. Parker and K. M. Short, "Reconstructing the keystream from a chaotic encryption," *IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications,* vol. 48, pp. 624-630, 2001.